2. Congruences and modular arithmetic

The notation for congruence is an invention of Gauss. It simplifies many calculations and arguments in number theory.

2.1. Definition and Basic Properties.

Definition 2.1.1. *Let m be a positive integer. For $a, b \in \mathbb{Z}$ we say that a is congruent to b modulo m and write $a \equiv b \pmod{m}$ iff $a - b$ is a multiple of m:*

$$a \equiv b \pmod{m} \iff m|(a-b).$$

Here m is called the modulus. If $m \nmid (a-b)$ then we write $a \not\equiv b \pmod{m}$.

For example, $-3 \equiv 18 \pmod{7}$ and $19 \not\equiv 1 \pmod{4}$. All even integers are congruent to $0 \pmod{2}$, while odd integers are congruent to $1 \pmod{2}$.

Congruence may be expressed in algebraic terms: to say $a \equiv b \pmod{m}$ is equivalent to saying that the cosets $a + m\mathbb{Z}$ and $b + m\mathbb{Z}$ of $m\mathbb{Z}$ in $\mathbb{Z}$ are equal.

The basic properties of congruence are summarized in the following lemmas.

Lemma 2.1.2. *For each fixed modulus m, congruence modulo m is an equivalence relation:*

(i) *Reflexive: $a \equiv a \pmod{m}$ for all $a \in \mathbb{Z}$;*

(ii) *Symmetric: $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$;*

(iii) *Transitive: If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.*

Lemma 2.1.3. *If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.*

The preceding result has the following interpretation. As well as $m\mathbb{Z}$ being a subgroup of the additive group $\mathbb{Z}$, it is also an ideal of the ring $\mathbb{Z}$, and hence there is a well-defined quotient ring $\mathbb{Z}/m\mathbb{Z}$. The lemma says that addition and multiplication in $\mathbb{Z}/m\mathbb{Z}$ are well-defined. We will return to this viewpoint in the next section.

Lemma 2.1.4. (i) *If $a \equiv b \pmod{m}$ then $ac \equiv bc \pmod{mc}$ for all $c > 0$;*
(ii) *If $a \equiv b \pmod{m}$ and $n|m$ then $a \equiv b \pmod{n}$.*

Lemma 2.1.5. *If $ax \equiv ay \pmod{m}$, then $x \equiv y \pmod{m/\gcd(a,m)}$.*
Two important special cases:
If $ax \equiv ay \pmod{m}$ and $\gcd(a,m) = 1$, then $x \equiv y \pmod{m}$.
If $ax \equiv ay \pmod{m}$ and $a|m$, then $x \equiv y \pmod{m/a}$.

Proposition 2.1.6. *Let $a, b \in \mathbb{Z}$. The congruence $ax \equiv b \pmod{m}$ has a solution $x \in \mathbb{Z}$ if and only if $\gcd(a,m)|b$. If a solution exists it is unique modulo $m/\gcd(a,m)$.*
In particular, when $\gcd(a,m) = 1$ the congruence $ax \equiv b \pmod{m}$ has a solution for every b, which is unique modulo m.

How to solve the congruence $ax \equiv b \pmod{m}$: Use the EEA to find d, u, v with $d = \gcd(a,m) = au + mv$. Check that $d|b$ (otherwise there are no solutions). If $b = dc$ then $b = auc + mvc$ so $x = uc$ is one solution. The general solution is $x = uc + tm/d = (ub + tm)/d$ for arbitrary $t \in \mathbb{Z}$.

Lemma 2.1.7. *Each integer a is congruent modulo m to exactly one integer in the set $\{0, 1, 2, \ldots, m-1\}$. More generally, let k be a fixed integer. Then every integer is congruent modulo m to exactly one integer in the set $\{k, k+1, k+2, \ldots, k+m-1\}$.*

Definition 2.1.8. *Taking $k = 0$, we obtain the system of* least non-negative residues modulo m*:* $\{0, 1, 2, \dots, m-1\}$*. Taking $k = -[(m-1)/2]$ gives the system of* least residues modulo m*; when m is odd this is $\{0, \pm 1, \pm 2, \dots, \pm(m-1)/2\}$, while when m is even we include $m/2$ but not $-m/2$. Any set of m integers representing all m residue classes modulo m is called a* residue system modulo m*.*

For example, when $m = 7$ the least non-negative residues are $\{0, 1, 2, 3, 4, 5, 6\}$ and the least residues are $\{-3, -2, -1, 0, 1, 2, 3\}$; for $m = 8$ we have least nonnegative residues $\{0, 1, 2, 3, 4, 5, 6, 7\}$ and least residues $\{-3, -2, -1, 0, 1, 2, 3, 4\}$.

2.2. The structure of $\mathbb{Z}/m\mathbb{Z}$.

Definition 2.2.1. *The* ring of integers modulo m *is the quotient ring $\mathbb{Z}/m\mathbb{Z}$. We will denote the group of units of $\mathbb{Z}/m\mathbb{Z}$ by U_m, and its order by $\varphi(m)$. The function $\varphi : \mathbb{N} \to \mathbb{N}$ is called* Euler's totient function *or* Euler's phi function*.*

Sometimes $\mathbb{Z}/m\mathbb{Z}$ is denoted $\mathbb{Z}_m$; however there is a conflict of notation here, since for prime p the notation $\mathbb{Z}_p$ is used to denote a different ring important in number theory, the ring of p-adic integers. *We will therefore not use this abbreviation!*

Informally we may identify $\mathbb{Z}/m\mathbb{Z}$ with the set $\{0, 1, 2, \dots, m-1\}$, though the elements of $\mathbb{Z}/m\mathbb{Z}$ are not integers but "integers modulo m": elements of the quotient ring $\mathbb{Z}/m\mathbb{Z}$. To be strictly correct, one should use the notation a, b, ... for integers and $\overline{a}$, $\overline{b}$, ... for their residues in $\mathbb{Z}/m\mathbb{Z}$. Then one has $\overline{a} = \overline{b}$ (in $\mathbb{Z}/m\mathbb{Z}$) iff $a \equiv b \pmod{m}$ (in $\mathbb{Z}$), and $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m-1}\}$. For simplicity we will not do this but use the same notation for an integer and its residue in $\mathbb{Z}/m\mathbb{Z}$.

So $\mathbb{Z}/m\mathbb{Z}$ is a finite ring with m elements, and its unit group U_m is a finite group under the operation of "multiplication modulo m".

Proposition 2.2.2. *Let $a \in \mathbb{Z}/m\mathbb{Z}$. Then $a \in U_m$ (that is, a is invertible modulo m) if and only if $\gcd(a, m) = 1$.*

Remark: Note that if $a \equiv a' \pmod{m}$ then $\gcd(a, m) = \gcd(a', m)$, since $a' = a + km$ for some k. Hence the quantity $\gcd(a, m)$ only depends on the residue of a modulo m.

We may use the Extended Euclidean Algorithm to detect whether or not a is invertible modulo m, and also to find its inverse a' if so, since if (x, y) is a solution to $ax + my = 1$ then $ax \equiv 1 \pmod{m}$ so we may take $a' = x$. For example, $\gcd(4, 13) = 1$ with $4 \cdot 10 - 13 \cdot 3 = 1$, so the inverse of 4 modulo 13 is 10. Here is a complete table of inverses modulo 13:

a	0	1	2	3	4	5	6	7	8	9	10	11	12
a'	-	1	7	9	10	8	11	2	5	3	4	6	12

It follows that $\varphi(m)$, the order of U_m, is equal to the number of residues modulo m of integers which are coprime to m. This is often given as the definition of $\varphi(m)$.

Corollary 2.2.3.

$$\varphi(m) = \left|\{a \mid 0 \le a \le m - 1 \quad \textit{and} \quad \gcd(a, m) = 1\}\right|.$$

Definition 2.2.4. *A* reduced residue system modulo m *is a set of $\varphi(m)$ integers covering the residue classes in U_m.*

Any set of $\varphi(m)$ integers which are all coprime to m, and no two of which are congruent modulo m, form a reduced residue system. The “standard” one is

$$\{a \mid 0 \le a \le m-1 \quad \text{and} \quad \gcd(a,m)=1\}.$$

For example, $U_6 = \{1,5\}$, $U_7 = \{1,2,3,4,5,6\}$ and $U_8 = \{1,3,5,7\}$, so that $\varphi(6)=2$, $\varphi(7)=6$ and $\varphi(8)=4$. Here are the first few values of $\varphi(m)$:

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	1
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	

Proposition 2.2.5. (1) *$\varphi(m)$ is even for $m \ge 3$;*
(2) *$\varphi(m) = m-1$ if and only if m is prime;*
(3) *Let p be a prime; then $\varphi(p^e) = p^{e-1}(p-1)$ for $e \ge 1$.*

We will use this to obtain a general formula for $\varphi(m)$ after the Chinese Remainder Theorem below, which will reduce the determination of $\varphi(m)$ for general m to the case of prime powers.

Arithmetic modulo m is much simpler when m is prime, as the following result indicates.

Theorem 2.2.6. *If p is a prime then $\mathbb{Z}/p\mathbb{Z}$ is a field. If m is composite then $\mathbb{Z}/m\mathbb{Z}$ is not a field, and not even an integral domain.*

Notation: To emphasize its field structure, $\mathbb{Z}/p\mathbb{Z}$ is also denoted $\mathbb{F}_p$, and the multiplicative group U_p is then denoted $\mathbb{F}_p^*$. It has order $p-1$, and is cyclic (see Theorem 2.6.1 below).

2.3. Euler’s, Fermat’s and Wilson’s Theorems.

Since U_m is a finite multiplicative group of order $\varphi(m)$ we immediately have the following as a consequence of Lagrange’s Theorem for finite groups.

Theorem 2.3.1. (a) **Euler's Theorem:** *Let m be a positive integer and a an integer coprime to m. Then*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

(b) **Fermat's Little Theorem:** *Let p be a prime and a an integer not divisible by p. Then*

$$a^{p-1} \equiv 1 \pmod{p};$$

moreover, for every integer a we have

$$a^p \equiv a \pmod{p}.$$

Fermat's Little Theorem can be used as a primality test. Let n be an odd integer which one suspects to be a prime; if $2^{n-1} \not\equiv 1 \pmod{n}$ then n is certainly not prime. Note that this has been proved without exhibiting a factorization of n. On the other hand, if $2^{n-1} \equiv 1 \pmod{n}$ it does not prove that n is prime! For example this holds with $n = 1729 = 7 \cdot 13 \cdot 19$. Such a number is called a pseudoprime to base 2. By using a combination of so-called bases (as here we used the base 2) one can develop much stronger "probabilistic primality tests".

Corollary 2.3.2. *In $\mathbb{F}_p[X]$ the polynomial $X^p - X$ factorizes as a product of p linear factors:*

$$X^p - X = \prod_{a \in \mathbb{F}_p} (X - a) \qquad \textit{in } \mathbb{F}_p[X].$$

Corollary 2.3.3. *[Wilson's Theorem] Let p be a prime. Then*

$$(p-1)! \equiv -1 \pmod{p}.$$

Remark: The converse to Wilson's Theorem also holds; in fact, for composite integers m greater than 4 we have $(m-1)! \equiv 0 \pmod{m}$ (exercise). But this is not useful as a primality test, since there is no way to compute the residue of $(m-1)! \pmod{m}$ quickly.
Example: Take $p = 13$. Then $(p-1)! = 12! = 479001600 = 13 \cdot 36846277 - 1$. A better way of seeing this is to write

$$12! \equiv 1 \cdot 12 \cdot (2 \cdot 7) \cdot (3 \cdot 9) \cdot (4 \cdot 10) \cdot (5 \cdot 8) \cdot (6 \cdot 11) \equiv 12 \equiv -1 \pmod{13}.$$

A similar trick, pairing each residue apart from ± 1 with its inverse, may be used to prove Wilson's Theorem directly. This works because ± 1 are the only residues modulo a prime which are their own inverse:

Proposition 2.3.4. *Let p be a prime. Then the only solutions to $x^2 \equiv 1 \pmod{p}$ are $x \equiv \pm 1$.*

Example: Let $m = F_5 = 2^{32} + 1 = 4294967297$. Check that $x = 1366885067$ satisfies $x^2 \equiv 1 \pmod{m}$. This proves that m is not prime. In fact, $m = ab$ where $a = 671 = \gcd(m, x-1)$ and $b = 6700417 = \gcd(m, x+1)$. Many modern factorization methods are based on this idea. Of course, one needs efficient ways to find solutions other than ± 1 to the congruence $x^2 \equiv 1 \pmod{m}$ where m is the (odd) composite number being factorized. There are several of these, which collectively go by the name of "quadratic sieve" methods.

2.4. Some Applications.

Proposition 2.4.1. *Let p be an odd prime. Then the congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.*

There are many other ways of proving the preceding Proposition. One is to use the fact that $\mathbb{F}_p^*$ is cyclic (Theorem 2.6.1), hence has elements of order d for all $d|(p-1)$, and an element a of order 4 satisfies $a^4 = 1$, $a^2 \neq 1$, so $a^2 = -1$. Alternatively, from Wilson's Theorem one can show that for all odd p,

$$(((p-1)/2)!)^2 \equiv -(-1)^{(p-1)/2} \pmod{p},$$

so when $p \equiv 1 \pmod{4}$ the number $a = ((p-1)/2)!$ satisfies $a^2 \equiv -1 \pmod{p}$.

As a corollary we can prove the result used earlier, that a prime of the form $4k+1$ may be written as a sum of two squares.

Theorem 2.4.2. *Let p be a prime such that $p \equiv 1 \pmod{4}$. Then there exist integers a and b such that $p = a^2 + b^2$.*

Remarks The first proof can be made constructive: given c satisfying $c^2 \equiv -1 \pmod{p}$, it is not hard to show that the element $a + bi = \gcd(c+i, p)$ in $\mathbb{Z}[i]$ satisfies $a^2 + b^2 = p$, so a single application of the Euclidean algorithm in $\mathbb{Z}[i]$ gives a solution.

The first proof also shows that the solution is essentially unique, up to permuting a and b and changing their signs. This follows from the fact that the factorization of p in $\mathbb{Z}[i]$ as $p = \pi\overline{\pi}$ with $\pi = a + bi$ is unique up to permuting the factors and multiplying them by units.

We finish this section with some more applications to the distribution of primes.

Proposition 2.4.3. (a) *There are infinitely many primes* $p \equiv 1 \pmod 4$.
(b) *There are infinitely many primes* $p \equiv 3 \pmod 4$.

Similarly, odd prime divisors of $n^4 + 1$ are $\equiv 1 \pmod 8$ and there are therefore infinitely many of those; odd prime divisors of n^8+1 are $\equiv 1 \pmod{16}$ so there are infinitely many of those; and so on. Next we have

Proposition 2.4.4. *Let* q *be an odd prime.*

(a) *Let* p *be a prime divisor of* $f(n) = n^{q-1} + n^{q-2} + \cdots + n + 1$. *Then either* $p = q$ *or* $p \equiv 1 \pmod q$.
(b) *There are infinitely many primes* $p \equiv 1 \pmod q$.

Using *cyclotomic polynomials* (for example, $f(n)$ above) one can show that there are infinitely many primes $p \equiv 1 \pmod m$ for any m. More generally *Dirichlet's Theorem on primes in arithmetic progressions* states that there are infinitely many primes $p \equiv a \pmod m$ whenever a and m are coprime: the general proof uses complex analysis!

2.5. **The Chinese Remainder Theorem or CRT.**

Proposition 2.5.1. *[Chinese Remainder Theorem for simultaneous congruences] Let* $m, n \in \mathbb{N}$ *be coprime. Then for every pair of integers* a, b *the simultaneous congruences*

$$\begin{aligned} x &\equiv a \pmod m \\ x &\equiv b \pmod n \end{aligned} \tag{2.5.1}$$

have a solution which is unique modulo mn.

More generally, if $d = \gcd(m,n)$ then the congruences (2.5.1) have a solution if and only if $a \equiv b \pmod{d}$, and the solution (when it exists) is unique modulo lcm$(m,n) = mn/d$.

To find the solution in the coprime case, write $1 = mu + nv$. Then we have the solution $x = mub + nva$ since $nv \equiv 1 \pmod{m}, \equiv 0 \pmod{n}$ while $mu \equiv 0 \pmod{m}, \equiv 1 \pmod{n}$.

Example: Let $m = 13$, $n = 17$. Then $1 = \gcd(13,17) = 52 - 51$ so the solution for general a, b is $x \equiv 52b - 51a \pmod{221}$.

The CRT says that there is a bijection between pairs $(a \mod m, b \mod n)$ and single residue classes $(c \mod mn)$ when m, n are coprime. This bijection is in fact a ring isomorphism:

Theorem 2.5.2. *[Chinese Remainder Theorem, algebraic form] Let $m, n \in \mathbb{N}$ be coprime. Then we have the isomorphism of rings*

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Restricting to units on both sides, we have the isomorphism of groups

$$U_{mn} \cong U_m \times U_n.$$

Both forms of the CRT extend to several moduli $m_1, m_2, \ldots, m_k$ provided that they are *pairwise* coprime. The second part of the proposition has the following important corollary: φ is a *multiplicative function*.

Proposition 2.5.3. *Let $m, n \in \mathbb{N}$ be coprime. Then $\varphi(mn) = \varphi(m)\varphi(n)$.*

Corollary 2.5.4. *Let $m \in \mathbb{N}$ have prime factorization*

$$m = \prod_{i=1}^{k} p_i^{e_i}$$

where the p_i are distinct primes and $e_i \geq 1$. Then

$$\varphi(m) = \prod_{i=1}^{k} p_i^{e_i-1}(p_i - 1) = m \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Examples: (1). $\varphi(168) = \varphi(8)\varphi(3)\varphi(7)$ (splitting 168 into prime powers) $= (8-4)(3-1)(7-1) = 4 \cdot 2 \cdot 6 = 48$. Alternatively, $\varphi(168) = 168 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{7}\right) = 168 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7} = 48$.
(2). $\varphi(100) = \varphi(4)\varphi(25) = 2 \cdot 20 = 40$.

One more property of $\varphi(m)$ will be useful later.

Proposition 2.5.5. *Let $m \in \mathbb{N}$. Then $\sum_{d|m} \varphi(d) = m$.*

The sum here is over all positive divisors of m. For example, when $m = 12$ we have

$$\begin{aligned} 12 &= \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) \\ &= 1 + 1 + 2 + 2 + 2 + 4. \end{aligned}$$

Applications of CRT: The CRT says that congruences to two coprime moduli are, in a sense, independent. Solving a general congruence to a general modulus reduces to solving it modulo prime powers, and then using CRT to “glue” the separate solutions together.

For example: solve $x^2 \equiv 1 \pmod{91}$. Since $91 = 7 \cdot 13$ we first solve separately modulo 7 and modulo 13, giving $x \equiv \pm 1 \pmod 7$ and $x \equiv \pm 1 \pmod{13}$ by an earlier proposition since 7 and 13 are prime. This gives four possibilities modulo 91:

$$\begin{aligned}
(+1 \mod 7, \quad +1 \mod 13) &\leftrightarrow (+1 \mod 91)\\
(+1 \mod 7, \quad -1 \mod 13) &\leftrightarrow (-27 \mod 91)\\
(-1 \mod 7, \quad +1 \mod 13) &\leftrightarrow (+27 \mod 91)\\
(-1 \mod 7, \quad -1 \mod 13) &\leftrightarrow (-1 \mod 91)
\end{aligned}$$

So the solutions are $x \equiv \pm 1 \pmod{91}$ and $x \equiv \pm 27 \pmod{91}$. To solve the second and third we use the method given above: write $1 = 7u + 13v = 14 - 13$, then $(a, b) = (1, -1)$ maps to $mub + nva = 14b - 13a = 14(-1) - 13(1) \equiv -27 \pmod{91}$.

Systematic study of various types of congruence now follows the following pattern. First work modulo primes; this is easiest since $\mathbb{Z}/p\mathbb{Z}$ is a field. Then somehow go from primes to prime powers. The process here (called "Hensel lifting") is rather like taking successive decimal approximations to an ordinary equation, and we will come back to this at the end of the module, in Chapter 5 on p-adic numbers. Finally, use the CRT to "glue" together the information from the separate prime powers.

2.6. **The structure of U_m.** The most important result here is that for prime p, the multiplicative group U_p $(= \mathbb{F}_p^*)$ is cyclic.

Theorem 2.6.1. *Let p be a prime. Then the group $U_p = \mathbb{F}_p^*$ is cyclic.*

Definition 2.6.2. *An integer which generates $U_p = \mathbb{F}_p^*$ is called a primitive root modulo p. If U_m is cyclic, then a generator of U_m is called a primitive root modulo m.*

When g is a primitive root modulo m, the powers $1, g, g^2, \dots, g^{\varphi(m)-1}$ are incongruent modulo m, and every integer which is coprime to m is congruent to exactly one of these. The other primitive roots are the g^k for which $\gcd(k, \varphi(m)) = 1$. So we have the following:

Corollary 2.6.3. *Let p be a prime. Then p has a primitive root, and the number of incongruent primitive roots modulo p is $\varphi(p-1)$. More generally, for every $d|(p-1)$ there are $\varphi(d)$ integers (incongruent modulo p) with order d modulo p.*

If m has a primitive root then there are $\varphi(\varphi(m))$ incongruent primitive roots modulo m.

Example: Let $p = 13$. Since $\varphi(p-1) = \varphi(12) = 4$ there are 4 primitive roots modulo 13. One is 2, since the successive powers of 2 modulo 13 are $1, 2, 4, 8, 3, 6, -1, \dots$. The others are the powers 2^k where $\gcd(k, 12) = 1$: taking $k = 1, 5, 7, 11$ gives the primitive roots $2, 2^5 \equiv 6, 2^7 \equiv 11, 2^{11} \equiv 7 \pmod{13}$.

As an application of primitive roots, we may give a simple proof of a result proved earlier, that when $p \equiv 1 \pmod 4$ then the congruence $x^2 \equiv -1 \pmod p$ has a solution. For let g be a primitive root modulo p, and set $a = g^{(p-1)/4}$. Then $a^2 \equiv g^{(p-1)/2} \not\equiv 1 \pmod p$, but $a^4 = g^{p-1} \equiv 1 \pmod p$, from which it follows that $a^2 \equiv -1 \pmod p$.

Theorem 2.6.4. *Primitive roots modulo m exist if and only if $m = 1, 2, 4,\ p^e$ or $2p^e$ where p is an odd prime and $e \geq 1$.*

Now if m is odd, with prime factorization $m = \prod_{i=1}^{k} p_i^{e_i}$, it follows that the group U_m is isomorphic to the product of cyclic groups of order $p_i^{e_i-1}(p_i - 1)$ for $1 \leq i \leq k$.

We have not determined the structure of U_{2^e} for $e \geq 3$; it turns out that while not cyclic, it is almost so: for $e \geq 3$, U_{2^e} is isomorphic to the product of cyclic groups of order 2 (generated by -1) and order 2^{e-2} (generated by 5).